UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/797,773 | 03/09/2004 | Mark Ammar Rayes | 50325-0865 | 4164 |

29989 7590 11/02/2007

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

| EXAMINER | |
|---|---|
| SHAIFER HARRIMAN, DANT B | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/02/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/797,773 | RAYES ET AL. | |
| | Examiner | Art Unit | |
| | Dant B. Shaifer - Harriman | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on *21 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

***Response to Amendment***

- ***Claims 1 – 22 & 24 – 31 are pending.***
- ***Claim 23 is cancelled.***
- ***Claims 27 – 31 are new claims.***
- ***Claims 1, 3-7, 14-16, 18-22, 26 are amended claims.***
- ***Claims 2, 8 – 13, 15 – 17, 24, and 25 are previously presented or original claims.***
- ***Claims 1 – 22 & 24 – 31 are rejected under 35 U.S.C. 112, ~~second~~ First paragraph and 35 U.S.C. 102e. Please see the detailed action below for further details.***
- ***Claim objections to claims 21 –23 are considered and are withdrawn.***
- ***Claim # 19 – Enablement Issue has been considered and withdrawn.***
- ***Claims 19, 22, 25 – Statutory Subject Matter have been considered and are with drawn.***
- Applicant's Arguments are moot in view of New ground of rejection.

**DETAILED ACTION**

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim(s) 22 & 25 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Please see In re Hyatt 708 F.2d 712,714-715, 218 USPQ 195, 197 (Fed. Cir. 1983), which discusses the error regarding single means plus function claims.

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim(s) 1 – 32 are rejected under 35 U.S.C. 102(e) as being taught by Renda et al. (US Patent # 7127524 B1).

Renda teaches:

Claim # 1. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device (Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network);

- determining a user identifier associated with the network device that has caused a security event in the network (Col. 9, lines 45 – 55 & Col. 10, lines 4 – 26 & Col. 23, lines 31 – 33 & Col. 24, lines 3 – 9, the examiner notes that he user identifier can take any form);

- causing the network device to acquire a new network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the examiner interprets "subset of addresses within a specified pool associated with suspected malicious network users," as merely a subset of generic IP addresses. );

- configuring one or more security restrictions with respect to the selected network address (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when

sufficient conditions are meant or granted access to network resources with exceptions).

Claim # 2 A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to

allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- correlating the security event information with network user information to result in determining the user identifier associated with the network device (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't

have the necessary privileges to use the network resources the users request will be blocked).

Claim # 3 A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to acquire the new network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the claim limitation "prompt a user to command the network device," the examiner interprets this as the device having an automated feature to accommodate the IP renew address

from the DHCP server, furthermore to one of ordinary skill in the art know that a common user will not know which IP address to choose from the DHCP server, based on the fact that the DHCP is also in contact with other network devices that must renew their IP addresses, therefore it isn't possible for user to initiate IP renew command, without knowing the total possible number of available IP addresses that can be used).

Claim # 4 A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to acquire the new network address comprises issuing a DHCP FORCE_RENEW message to the network device (Col. 14, lines 55 – 67 & Col.

15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the, claims limitation "DHCP FORCE_RENEW," is merely the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well).

Claim #5 A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step

of causing the network device to acquire the new network address comprises prompting the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well).

Claim # 6 A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step

of causing the network device to acquire the new network address comprises waiting for expiration of a lease for a current network address of the network device (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well).

Claim # 7 A method as recited in Claim 1, wherein

- the step of causing the network device to acquire the new network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52 & Col. 18, lines 52 - 61, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the examiner interprets "subset of addresses within a specified pool associated with suspected malicious network users," as merely a subset of generic IP addresses or a "special IP subnet").

Claim # 8 A method as recited in Claim 7, further comprising

- the step of publishing information describing characteristics of the special IP subnet to network service providers (Col. 16, lines 23 – 29, the examiner notes that the system administrator is considered the network service provider, furthermore the system administrator will know the necessary capabilities of its equipment that is being used on its network).

Claim # 9 A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to

resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions, furthermore the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources).

Claim # 10 A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device

to permit entry of traffic only for a MAC address that is bound to the selected network address (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions, furthermore the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources).

Claim # 11. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked).

Claim # 12. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if not, removing the user from the elevated risk group (Col. 10, lines 54 – 67 & Col. 11, lines 1 – 8, the examiner notes that the if the user is on a "do not allow list," then the user request and associated network information is deleted from the system).

Claim # 13. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated

with a trusted customer of a network service provider (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21 & Col. 9, lines 3 – 8, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, if a user doesn't have the necessary privileges to use the network resources the users request will be blocked, otherwise if the user has committed a malicious act, the user might still be granted access to the network with exceptions ).

Claim # 14. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device (Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network);

- receiving information identifying a security event in the network; correlating the security event information with network user information to result in determining a network user associated with the network device, that caused the

security event (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a subset of addresses within a specified pool associated with

suspected malicious network users:

- configuring one or more security restrictions with respect to the selected network address (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions);

- determining whether a malicious act caused the security event (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and

privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers,

IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group (Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user

requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked).

Claim # 15. A method as recited in Claim 14, wherein

- placing the user identifier in an elevated risk security group further comprises the step of forcing the device to acquire the new network address from a specified group of network addresses that is reserved for users associated with elevated user risk (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the

examiner interprets "specified group of network addresses that is reserved for users associated with elevated user risk," as merely a subset of generic IP addresses).

Claim # 16. A method as recited in Claim 15, wherein forcing the user to acquire the new network address comprises the steps of:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the

examiner interprets "specified group of network addresses that is reserved for users associated with elevated user risk," as merely a subset of generic IP addresses);

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must

also have the proper privileges to renew as well);

(b) issuing a DHCP FORCE_RENEW message to the network device (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the, claims limitation "DHCP FORCE_RENEW," is merely the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well);

(c) prompting the network device to request a new network address using DHCP(Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the

examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well);

(d) waiting for expiration of a lease for a current network address of the network
device (Col. 15, lines 67 & Col. 16, lines 1 - 3).

Claim # 17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps

of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address (Col. 24, lines 58 – 62 & Col. 27, lines 52 – 57 & Col. 21, lines 58 – 65 & Col. 19, lines 33 – 52, the examiner notes that the master access controller # 222, has a master list of MAC addresses, which examiner regards as a " Access control list, or ACL," that it checks to see whether or not to allow the requesting user access to the network);

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the selected network address (Col. 25, lines 63 – 67 & Col. 26, lines 1- 2, the examiner notes that the master access controller # 222, may use the source port

number to identify the user requesting access to the network, furthermore, the master access controller #222 has a master list of MAC addresses, which examiner regards as a " Access control list, or ACL," that it checks to see whether or not to allow the requesting user access to the network).

Claim # 18. A computer-readable medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- in a security controller that is coupled, through a network, to a network device (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the examiner considers the "memory or storage drive" located with in a generic computer as

"computer readable medium," with references invention located thereon, furthermore, (Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network );

- determining a user identifier associated with the network device that has caused a security event in the network (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the examiner considers the "memory or storage drive" located with in a generic computer as "computer readable medium," with references invention located thereon, furthermore, (Col. 9, lines 45 – 55 & Col. 10, lines 4 – 26 & Col. 23, lines 31 – 33 & Col. 24, lines 3 – 9, the examiner

notes that he user identifier can take any form);

- causing the network device to acquire a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the examiner considers the "memory or storage drive" located with in a generic computer as "computer readable medium," with references invention located thereon, furthermore, (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore, the examiner notes that the examiner interprets "subset of addresses within a specified

pool associated with suspected malicious network users," as merely a subset of generic IP addresses. ); and

- configuring one or more security restrictions with respect to the selected network address (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the examiner considers the "memory or storage drive" located with in a generic computer as "computer readable medium," with references invention located thereon, furthermore, (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions).

Claim # 19 An apparatus, comprising:

- in a security controller that is coupled, through a network, to a network device (Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network);

- means for determining a user identifier associated with the network device that has caused a security event in the network (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 9, lines 45 – 55 & Col. 10, lines 4 – 26 & Col. 23, lines 31 – 33 & Col. 24, lines 3 – 9, the examiner notes that he user identifier can

take any form);

- means for causing the network device to acquire a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore, the examiner notes that the examiner interprets "subset of addresses within a specified pool associated with suspected malicious network users," as merely a subset of generic IP

addresses); and

- means for configuring one or more security restrictions with respect to the selected network address (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions).

Claim # 20.An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom (Col.7, lines 15 – 23 & Col. 18, lines 52 – 61, the examiner notes that the network interface, interfaces between a sub-network and the network (i.e. the public internet ));

- a processor (Col. 6, lines 4 – 11, the examiner notes that the references invention is embodied in software instructions and executed by a process on a general purpose computer );

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

- in a security controller that is coupled, through a network, to a network device (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48,

the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network);

- determining a user identifier associated with a-the network device that has caused a security event in a-the network (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 9, lines 45 – 55 & Col. 10, lines 4 – 26 & Col. 23, lines 31 – 33 & Col. 24, lines 3 –

9, the examiner notes that he user identifier can take any form);

- causing the network device to acquire a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore, the examiner notes that the examiner interprets "subset of addresses within a specified pool associated with suspected malicious

network users," as merely a subset of generic IP addresses); and

- configuring one or more security restrictions with respect to the selected network address (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, (Col. 8, lines 48 – 58 & Col. 9, lines 3 – 8, the examiners notes that the user can be granted access to resources (i.e. website or websites ), when sufficient conditions are meant or granted access to network resources with exceptions).

Claim # 21. A computer-readable medium as recited in Claim 18, further comprising

- instructions for performing the steps as recited in any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13 (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore please see any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13 above for further detail).

Claim # 22. An apparatus as recited in Claim 19, further comprising

- means for performing the steps as recited in any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13 (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references

invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore please see any of Claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, or 13 above for further detail).

Claim # 24. A computer-readable medium

- carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps as recited in any of Claims 14, 15, 16, or 17 (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore please see any of Claims 14, 15, 16, or 17

above for further detail).

Claim # 25. An apparatus comprising

- means for performing the functions recited in the steps of any of Claims 14, 15, 16, or 17 (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore please see any of Claims 14, 15, 16, or 17 above for further detail).

Claim # 26. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom (Col.7, lines 15 – 23 & Col. 18, lines 52 – 61, the examiner notes that the network interface, interfaces between a sub-network and the network (i.e. the public internet);

- a processor (Col. 6, lines 4 – 11, the examiner notes that the references invention is embodied in software instructions and executed by a process on a general purpose computer); and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out:

- in a security controller that is coupled, through a network, to a network device (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is

embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 8, lines 48 – 58 & Col. 7, lines 66 – 67, Col. 8, lines 1 – 14 & Col. 24, lines 13 – 23 & Col. 25, lines 3 – 16, Col. 25, lines 63 – 67 & Col. 26, lines 1-2 the examiner notes that the master controller can be the security controller both of which decide whether or not to allow a user or a client access to resources on the network);

- receiving information identifying a security event in the network (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 &

Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 7, lines 63 – 67

& Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a subset of addresses within a

specified pool associated with suspected malicious network users (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the examiner interprets "specified group of network addresses that is reserved for users associated with elevated user risk," as merely a subset of generic IP addresses );

configuring one or more security restrictions with respect to the selected network address:

- determining whether a malicious act caused the security event (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user

requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked );

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1 – 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed

user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 7, lines 63 – 67 & Col. 8, lines 1 –14 & Col. 8, lines 48 – 58 & Col. 9, lines 45 – 47 & Col. 10, lines 44 – 48 & Col. 10, lines 54 – 64 & Col. 11, lines 1

– 7 & Col. 24, 13 – 23 & Col. 25, lines 3 – 16 & Col. 26, lines 6 – 21, the examiner notes that the authentication server or the master access controller or the Privilege manger, all contain allowed user source IP addresses and destination addresses and privilege records, user identifiers, IP device identifiers that are necessary for the determination on whether or not to allow a user requesting access to the network resources, a user doesn't have the necessary privileges to use the network resources the users request will be blocked ).

Claim # 27. The apparatus of claim 26, wherein

- the instructions for placing the user identifier in an elevated risk security group further comprise instructions which when executed cause forcing the user to acquire a new network

address from a specified group of network addresses that is reserved for users associated with elevated user risk (Col. 6, lines 4 – 18 & Col. 6, lines 34 – 48, the examiner notes that the references invention is embodied in software instructions or code that is implemented in a general purpose computer, furthermore, Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the examiner interprets "specified group of network addresses that is reserved for users associated with elevated user risk," as merely a subset of generic IP addresses );

Claim # 28. The apparatus of claim 27, wherein the instructions which when executed cause forcing the user to acquire a new network address comprise further instructions which when executed cause:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk (Col. 16, lines 15 – 37 & Col. 35, lines 29 – 52, the examiner notes that the access controller # 222 in figure 2A or the DHCP server or manager # 284, will consider the network device as a suspected malicious user until the user is determined to have access based on privileges granted, furthermore the examiner notes that the examiner interprets "specified group of network addresses

that is reserved for users associated with elevated user risk," as merely a subset of generic IP addresses);

performing any one of the steps of:

(e) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must

also have the proper privileges to renew as well);

(f) issuing a DHCP FORCE_RENEW message to the network device (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the, claims limitation "DHCP FORCE_RENEW," is merely the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well);

(g) prompting the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the

examiner notes that the DHCP server forcing the user or networked device to change IP addresses if it is unable to operate in "real IP mode," meaning the IP address that the networked device is already using is being used by another networked device on the same network, so it must renew if it wants to use the networked resources, the network resources must also have the proper privileges to renew as well);

(h) waiting for expiration of a lease for a current network address of the network device (Col. 15, lines 67 & Col. 16, lines 1 - 3).

Claim # 29. The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address (Col. 24, lines 58 – 62 & Col. 27, lines 52 – 57 & Col. 21, lines 58 – 65 & Col. 19, lines 33 – 52 & Col. 8, lines 65 - 67, the examiner notes that the master access controller # 222, has a master list of MAC addresses, which examiner regards as a " Access control list, or ACL," that it checks to see whether or not to allow the requesting user access to the network);

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the selected network address (Col. 25, lines 63 – 67 & Col. 26, lines 1- 2, the examiner notes that the master access controller # 222, may use the source port number to identify the user requesting access to the

network, furthermore, the master access controller #222 has a master list of MAC addresses, which examiner regards as a " Access control list, or ACL," that it checks to see whether or not to allow the requesting user access to the network).

Claim # 30 The apparatus of claim 20, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the instructions which when executed cause the network device to receive a network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP (Col. 14, lines 55 – 67 & Col. 15, lines 1 – 67 & Col. 16, lines 1 – 37 & Col. 35, lines 29 – 56, the examiner notes that the claim limitation "prompt a user to command the network

device," the examiner interprets this as the device having an automated feature to accommodate the IP renew address from the DHCP server, furthermore to one of ordinary skill in the art know that a common user will not know which IP address to choose from the DHCP server, based on the fact that the DHCP is also in contact with other network devices that must renew their IP addresses, therefore it isn't possible for user to initiate IP renew command, without knowing the total possible number of available IP addresses that can be used).

Claim # 31. The apparatus of claim 20, wherein

- instructions which when executed cause the network device to receive a network address comprise instructions which when executed cause providing the network device with an

IP address that is selected from a plurality of IP addresses within a special IP subnet (Col. 6, lines 4 – 14 & Col. 6, lines 62 - 66, the examiner notes that the references invention can be implemented in code or program software instructions that is executed by a processor).

***Conclusion***

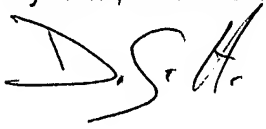
Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER